

United States Senate
WASHINGTON, DC 20510

December 8, 2000

Mr. David Strauss
Executive Director
Pension Benefit Guaranty Corporation
1200 K Street NW
Washington, DC 20005

Via fax: (202)326-

Dear Mr. Strauss:

Thank you very much for transmitting the final monthly report of the Pension Benefit Guaranty Corporation (PBGC) on the implementation of the PBGC's information security corrective action plan. We appreciate your regular and timely monthly reports and are glad to see much progress in tightening computer security. We hope you will convey our appreciation to your hard-working computer staff.

Of all the items in the action plan, the ones that provide continuing interest and value undoubtedly are the regular review by an outside firm and the regular seminars for PBGC staff on the importance of computer security. Periodic assessments by specialists who monitor new developments in the hacker world, and frequent reminders to PBGC staff that they must maintain their vigilance, are vital to ensuring that computer security remains strong. Hackers and mischief-makers are continuously attempting to upgrade their weapons, and agencies must continuously seek to stay one step ahead of them.

In fact, we share the concern raised by the Inspector General (IG) in a November 30, 2000 letter (attached) that PBGC needs to conduct security awareness training more often than annually. As the IG notes, social engineering vulnerabilities are particularly sensitive. If employees are not frequently reminded of the dangers, it is easy to fall back into old habits that compromise security. Annual reminders do not seem frequent enough to prevent such relapses.

Please provide us with your views on the IG's concern on this point. Also, we would like your response to the IG's concern about technical security standards for various PBGC computer platforms. As the IG states, on-going monitoring of compliance with standards is also vital.

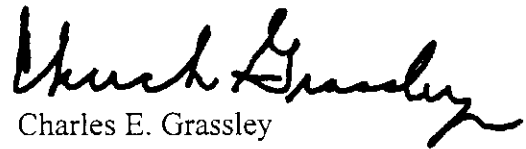
Mr. David Strauss
Page Two

Finally, we would welcome additional updates, from time to time as developments warrant, on additional measures taken by the PBGC to protect sensitive pensioner data from looting by unauthorized users.

Sincerely,



Christopher S. Bond
Chairman
Committee on Small Business



Charles E. Grassley
Chairman
Special Committee on Aging

cc: Wayne Robert Poll,
PBGC Inspector General



Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

Office of Inspector General

November 30, 2000

The Honorable Christopher S. Bond
Chairman, Committee on Small Business
United States Senate
Washington, D.C. 20510

The Honorable Charles E. Grassley
Chairman, Special Committee on Aging
United States Senate
Washington, D.C. 20510

Dear Senator Bond and Senator Grassley:

We write to update your committee staffs on Pension Benefit Guaranty Corporation's (PBGC) efforts to correct identified security vulnerabilities reported in a Network Penetration Study (October 8, 1999) published by the Office of Inspector General (OIG). A January 11, 2000 letter from your Committees to Executive Director David Strauss stated that PBGC must complete corrective action on all ten (10) high-level findings by September 30, 2000. In addition, you asked the OIG, in a separate communication, to monitor PBGC's progress and report its resolution after the scheduled completion date.

To verify PBGC's corrective actions, we attended executive committee status meetings, interviewed PBGC management and technical staff, and reviewed system data. In addition, we compared findings presented in the Network Penetration Study with PBGC's corrective action plans. PBGC reported monthly to your committees their progress in implementing the corrective action plans. We evaluated PBGC's assertions and follow-up actions taken.

Our oversight activities found that PBGC has taken adequate action on all high-level findings presented in the Network Penetration Study, and we have validated the actions as appropriate. We also cross-linked twenty-three (23) recommendations resulting from the penetration testing to the high-level findings and determined that PBGC has taken proper steps toward implementing each of the twenty-three (23) recommendations.

However, we noted that two findings, although considered complete by PBGC, would require continuous attention in the future. Below, you will find the two findings with our comments:

- *The development and implementation of an organizational information security policy that addresses security configurations and standards, policy and procedures, user education, and enforcement of security policies.*

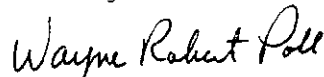
PBGC issued information security policy corporate wide and enhanced user security awareness through training to satisfy OIG's finding. However, our review shows that PBGC still needs to implement technical security standards for the various computer platforms it uses, and maintain a viable program for monitoring compliance before its information security policy is complete.

- *Development of security awareness program for PBGC information systems users and administrators.*

Our evaluation found that PBGC developed and conducted security awareness training for both federal employees and contractors to meet the OIG finding. However, PBGC should broaden its security awareness program to include a more proactive and standardized approach. We believe that just relying on an annual awareness training for employee and contractors will create a security gap, in view of the social engineering success the penetration testing team demonstrated in FY 1999.

Overall, a review of PBGC's actions to implement its corrective action plan has essentially satisfied our reported security weaknesses and will effectively strengthen PBGC's overall security program. As you have requested, we intend to monitor PBGC's security program and conduct additional security reviews to test the effectiveness of its controls.

Sincerely,



Wayne Robert Poll
Inspector General

cc: David Strauss, Executive Director
Pension Benefit Guaranty Corporation

Paul Connelly, Partner
PricewaterhouseCoopers